

UNITED STATES DISTRICT COURT

for the
Western District of North CarolinaFILED
ASHEVILLE, N.C.
MAY 28 2019
U.S. DISTRICT COURT
W. DIST. OF N.C.

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)
 a red Apple iPhone XR (A1984) telephone number
 828-242-0279, IMEI number 35734-50965-24572

Case No.

1:19-mj-54

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
 See attachment A on Corresponding affidavit

located in the Western District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

This warrant authorizes the forensic examination of the above described cell phone for the purpose of identifying the electronically stored information described in Attachment B of the corresponding affidavit.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

evidence of a crime;
 contraband, fruits of crime, or other items illegally possessed;
 property designed for use, intended for use, or used in committing a crime;
 a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

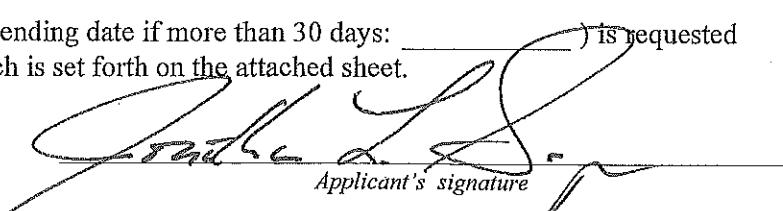
Code Section
18 USC 1951

Offense Description
Robbery/Interstate Commerce

The application is based on these facts:
 See Affidavit

Continued on the attached sheet.

Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
 under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


 Jonathan L. Scruggs, FBI Task Force Officer

Printed name and title

Sworn to before me and signed in my presence.

Date:

5/28/2019


 W. Carleton Metcalf, U.S. Magistrate Judge, WDNC

Printed name and title

City and state: Asheville, NC

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA

FILED
ASHEVILLE, N.C.
MAY 28 2019
U.S. DISTRICT COURT
W. DIST. OF N.C.

IN THE MATTER OF THE SEARCH OF:
A red iPhone XR (A1984), telephone number
828-242-0279, IMEI Number 35734-50965-
24572 in the custody of the Buncombe County
Sheriff's Office

Case No. 1:19-mj-54

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Jonathan L. Scruggs, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for a red Apple iPhone XR, telephone number 828-242-0279, and bearing IMEI Number 35734-50965-24572. The aforementioned device is known to be in the custody of the Buncombe County Sheriff's Office. I also seek the extraction from that property of electronically stored information described in Attachment B. Based on my investigation, I believe there is probable cause to search this device for violations of 18 U.S.C. § 1951.

2. I am a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI), and have been since June 05, 2017. I am currently assigned to the Asheville Resident Agency of the Charlotte, North Carolina field office. As a Task Force Officer, I am a law enforcement officer of the United States as defined by Section 2510(7) of Title 18, United States Code (U.S.C.). As a Task Force Officer, I have conducted and participated in a variety of criminal

investigations, including investigations associated with murder, bank robberies, armed robberies, fugitives, financial crimes, computer crimes, as well as other violent criminal acts.

3. The facts in this affidavit come from my personal observations, my training experience, and information obtained from other law enforcement officers and witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE SEIZED AND EXAMINED

4. The property to be searched is a red iPhone XR (A1984), telephone number 828-242-0279, IMEI Number 35734-50965-24572. The Device is currently in the custody of the Buncombe County Sheriff's Office.

5. The applied-for warrant would authorize the transfer of the device from the Buncombe County Sheriff's Office to the Federal Bureau of Investigation, from wherever the Device may be stored. The warrant would also allow for the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

RELEVANT STATUTES

6. **18 U.S.C § 1951** prohibits the interference of commerce by threats or violence.

In relevant part, it states:

(a) Whoever in any way or degree obstructs, delays, or affects commerce or the movement of any article or commodity in commerce, by robbery or extortion or attempts or

conspires so to do, or commits or threatens physical violence to any person or property in furtherance of a plan or purpose to do anything in violation of this section shall be fined under this title or imprisoned not more than twenty years, or both.

(b) As used in this section—

(1) The term “robbery” means the unlawful taking or obtaining of personal property from the person or in the presence of another, against his will, by means of actual or threatened force, or violence, or fear of injury, immediate or future, to his person or property, or property in his custody or possession, or the person or property of a relative or member of his family or of anyone in his company at the time of the taking or obtaining.

(2) The term “extortion” means the obtaining of property from another, with his consent, induced by wrongful use of actual or threatened force, violence, or fear, or under color of official right.

(3) The term “commerce” means commerce within the District of Columbia, or any Territory or Possession of the United States; all commerce between any point in a State, Territory, Possession, or the District of Columbia and any point outside thereof; all commerce between points within the same State through any place outside such State; and all other commerce over which the United States has jurisdiction.

TECHNICAL TERMS

7. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images.

Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- d. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

8. Based on my training, experience, and research, I know that the MOBILE DEVICE has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, and GPS navigation device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

9. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

10. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

PROBABLE CAUSE

11. On May 19, 2019 the Buncombe County Sheriff's Office (BCSO) initiated an investigation following an armed robbery that occurred at the AT&T Wireless store located at 335 Airport Road, Arden, North Carolina 28704. During the course of the investigation, Detectives of the BCSO were provided video surveillance footage of the interior of the store at the time the alleged crime ensued. Video imagery allowed the detectives to observe two black males entering the store, one wearing red shoes, black pants with a white stripe aligned vertically up both legs of the pants, black hooded sweatshirt, toboggan and gloves, along with a red face covering. The other assailant appeared to be a black male clad in a black Nike hooded sweatshirt, tan pants, black sandals, green and black gloves armed with a handgun.

12. According to the employee present inside the store at the time of the robbery, the assailant armed with the handgun pointed it at him and instructed him to lay down on the floor. The employee stated during this time the register was opened and contents removed. According to the employee, he was then instructed to access a locked door leading to the storage area where new, unsold cellular phones are kept. The assailants then placed cellular phones into a black and grey bag subsequently leaving the store.

13. The following day, May 20, 2019, shortly after 9:00 am the Verizon Wireless store located at 1602 Four Seasons Boulevard, Hendersonville, North Carolina 28792 was also robbed at gunpoint. According to information provided by officers and investigators with the Hendersonville Police Department (HPD), an employee of the Verizon Store activated a Global Positioning System (GPS) tracking device disguised as a cellular telephone while the robbery

was in progress. The employee was able to activate the GPS tracker and secrete it into the bag of cellular phones stolen and carried away by the assailants. Information from law enforcement responders to the Hendersonville Verizon store revealed the assailants utilized a silver Hyundai vehicle bearing Florida registration plate number AEZX41.

14. Once the HPD was made aware of the robbery, a Be On the Look Out (BOLO) notification was sent to surrounding law enforcement jurisdictions, containing the suspect and vehicle information from the robbery. The HPD began receiving GPS locations updates every six seconds from the device taken by the assailants. The aforementioned GPS updates directed deputies from the BCSO to set up and interdict the suspect vehicle on Charlotte Highway in the vicinity of Reynolds High School.

15. Sergeant Matthew Howie (Sgt. Howie) of the BCSO Patrol Division observed a silver Hyundai bearing Florida Registration Plate AEZX41, and attempted to stop the vehicle. The operator of the vehicle then fled from the active pursuit and exited onto Fairview Road in the Oakley Community of Asheville with BCSO Patrol deputies in pursuit. Shortly thereafter, the suspect vehicle came to rest behind 344 Fairview Road.

16. BCSO observed a black male wearing black clothing complete with red shoes and a vertically aligned white stripe on the legs of the trousers running away from the vehicle. Sgt. Howie pursued the suspect on foot, apprehending him a short distance from the suspect vehicle. The suspect would be identified as Kristoff Michael Hunter (Hunter). A subsequent search of the Hunter's direct path of flight revealed a Beretta 92F nine-millimeter pistol and a red iPhone very

close to one another, and very close to the captioned vehicle. After being apprehended by Sgt. Howie, Hunter asked Sgt. Howie if his phone had been located. Sgt. Howie asked Hunter what the phone he was referencing looked like, and Hunter advised him it was a red iPhone.

17. A state search warrant executed on the vehicle by detectives of the BCSO revealed numerous unopened new cellular telephones along with Apple watches that were listed on inventory reports provided by both the AT&T Store as well as the Verizon Store in Hendersonville.

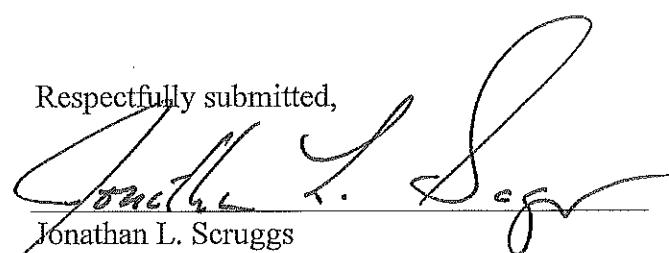
18. Both the AT&T Store as well as the Verizon Store are believed to conduct business that affects interstate and foreign commerce.

19. Based on my review of the facts and circumstances of this case, I believe there is sufficient probable cause to believe the Device requested to be searched contains evidence of the planning, preparation, and commission of the alleged crime captioned in 18 U.S.C. § 1951.

CONCLUSION

20 I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,


Jonathan L. Scruggs
Task Force Officer
Federal Bureau of Investigation

Reviewed by AUSA John D. Pritchard on May 28, 2019.

Subscribed and sworn to before me on May 28, 2019.



W. CARLETON METCALF
UNITED STATES MAGISTRATE JUDGE
WESTERN DISTRICT OF NORTH CAROLINA

ATTACHMENT A

One (1) red Apple iPhone XR, telephone number 828-242-0279, believed to be owned by Kristoff Michael Hunter, known to be in the custody of the Buncombe County Sheriff's Office. This warrant authorizes the transfer of the device from the Buncombe County Sheriff's Office and the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. § 1951.
2. All electronic files containing evidence of the planning, preparation, and execution of the robbery as defined in 18 U.S.C. § 1951 and records or other items which evidence ownership or use of computer that is currently saved on the MOBILE DEVICE.
3. Records, documents, writings, and correspondences with others pertaining to the planning, preparation, and execution of the robbery as defined in 18 U.S.C. § 1951.
4. Any and all, photographs, letters, written narratives and computer text files or electronic matter to show or evidence of the planning, preparation, and execution of the robbery as defined in 18 U.S.C. § 1951
5. Electronic mail, chat logs, and electronic messages, offering to assist in the planning. Preparation, and execution of the robbery as defined in 18 U.S.C. § 1951.
6. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, letters, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.
7. Storage combinations, and passwords, which indicate any other storage containers

or facilities that could contain evidence of the planning, preparation, and execution of the robbery noted as a violation of 18 U.S.C. § 1951

8. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.